IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. 852,654.047192 USDT TOKENS SEIZED FROM THE CRYPTOCURRENCY WALLET ADDRESS IDENTIFIED BY TY12X97szmYzYAmYLsh86cbYfh9psufgeV, 105,553.680342 USDT TOKENS SEIZED FROM THE CRYPTOCURRENCY WALLET ADDRESS IDENTIFIED BY TA86m1veBthXyvXcN1mDixgYNXChkMjhh, and 1,013,192.066449 USDT TOKENS SEIZED FROM THE CRYPTOCURRENCY WALLET ADDRESS IDENTIFIED BY TPMVocf6Rv6bMLnRMX4RXoriiTbT9P82k2, Defendants *in Rem.*	)	Civil Case No. 1:25-cv- 559

VERIFIED COMPLAINT FOR FORFEITURE IN REM

COMES NOW the plaintiff, United States of America, by and through its counsel, Erik S. Siebert, United States Attorney for the Eastern District of Virginia and by Annie Zanobini, Assistant United States Attorney, and brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

NATURE OF THE ACTION

1. The United States brings this action *in rem* seeking the forfeiture of all right, title and interest in the defendants in rem identified in the case caption above (together, the "Defendant Property"). The Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) and (a)(1)(A).

THE DEFENDANTS IN REM

2. Defendant 852,654.047192 USDT tokens was seized from a cryptocurrency wallet address identified by TY12X97szmYzYAmYLsh86cbYfh9psufgeV and is currently held in a cryptocurrency wallet address controlled wallet address controlled by the Federal Bureau of Investigation ("FBI") in the Eastern District of Virginia.

3. Defendant 105,553.680342 USDT Tokens was seized from a cryptocurrency wallet address identified by TA86m1veBthXyvXcN1mDixgYNXChkMjhhZ and is currently held in a cryptocurrency wallet address controlled wallet address controlled by the FBI in the Eastern District of Virginia.

4. Defendant 1,013,192.066449 USDT Tokens was seized from a cryptocurrency wallet address identified by TPMVocf6Rv6bMLnRMX4RXoriiTbT9P82k2 and is currently held in a cryptocurrency wallet address controlled by the FBI in the Eastern District of Virginia.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a) and (b).

4. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. §

1355(b)(1)(B) with reference to 28 U.S.C. § 1395(b) because the Defendant Property is located in the Eastern District of Virginia and under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

5. Venue is proper in this judicial district under 28 U.S.C. § 1355(b)(1)(B) with reference to 28 U.S.C. § 1395(b) because the Defendant Property is located in the Eastern District of Virginia and under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

BASIS FOR FORFEITURE

6. 18 U.S.C. § 981(a)(1)(C) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a specified unlawful activity ("SUA"), as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA. 18 U.S.C. § 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of Title 31 of the U.S. Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343.

6. 18 U.S.C. § 981(a)(1)(A) provides for the forfeiture of any property, real or personal, involved in a violation or attempted violation of 18 U.S.C. § 1956, or any property traceable to such property.

STATEMENT OF FACTS

7. The FBI seized the Defendant Property from criminals involved in investment fraud scams. The United States of America seeks to lawfully forfeit the Defendant Property to

punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities and to recover assets that may be used to compensate victims.[1]

A. Background on cryptocurrency

8. **Virtual Currency:** Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently one of the most popular virtual currencies in use.

9. **Virtual Currency Address:** Virtual currency addresses are the digital locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers. It is possible to "swap", or otherwise, exchange cryptocurrencies by using Decentralized Exchanges (DEXs). DEXs allow for the swapping of one cryptocurrency for another by keeping large liquidity pools of various cryptocurrency types, which users can then swap between for a nominal fee. Unlike Centralized Cryptocurrency Exchanges, DEXs are not custodial, and allow for these swaps through the use of smart contracts, and therefore avoid the need for a third party to ever have custody of the cryptocurrencies being swapped. A DEX does not collect Know Your customer (KYC) information.

10. **Virtual Currency Exchange:** Virtual currency exchanges, such as Crypto.com are trading and/or storage platforms for virtual currencies. Many exchanges also store their

[1] *See* United States Asset Forfeiture Program, *Our Mission*, https://www.justice.gov/afp.

customers' virtual currency in virtual currency accounts. These virtual currency accounts are commonly referred to as wallets and can hold multiple virtual currency addresses.

11. **Blockchain:** Many virtual currencies, including Ether, publicly record all their transactions on what is known as a blockchain. The blockchain is a distributed public ledger containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. Due to the international nature of virtual currencies, most blockchain explorers operate using the Coordinated Universal Time (UTC) Zone. The times/dates used in this complaint are also based on the UTC time zone.

12. **Blockchain Analysis:** While the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity.

13. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, Tether (USDT) is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

14. **Tether (USDT):** Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

15. **Ether:** Ether ("ETH") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH.

16. **Bitcoin:** Bitcoin (or "BTC") is a type of virtual currency. Unlike traditional, government-controlled currencies (i.e., fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin's software. Those computers are called network nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

B. The Investment Fraud Scheme

17. This complaint involves criminal syndicates operating cryptocurrency investment fraud schemes. The scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S. victims. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal their money.

18. This type of scam involves scammers spending significant time getting to know and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds via wire transfer or through a provided

cryptocurrency deposit address. While the scammers prefer cryptocurrency deposits, they will also accept bank wires if the victim cannot transfer cryptocurrency.

19. As part of the scheme to defraud, the victims are told that they can expect to make a sizeable return on their investments. As investments are made, the spoofed websites falsely displayed a significant increase in the victim's account balance, which encouraged the victim to continue making investments. When the victim attempted to make a withdrawal, the scammers often attempted to coerce the victims to send even more funds. These tactics included requesting additional deposits due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempted to solicit additional investments from the victims, the victims were unable to recover their investment.

20. The criminals then move the victim funds beyond reach of law enforcement, typically by using non-custodial or "private" wallets that law enforcement cannot attribute using legal process or blockchain analysis alone; by transferring victim funds through multiple wallets before those funds reach a consolidation wallet; and by commingling victim funds with other funds in a consolidation wallet and sometimes then further transferring the funds to additional "downstream" wallets. Criminals frequently liquidate their cryptocurrency fraud proceeds by using "brokers" who agree to buy the cryptocurrency in exchange for other currency, including fiat currency.

C. The Scheme and the victim

21. The victim, a resident of the Eastern District of Virginia, reported information to the FBI as well as Loudoun County Sheriff's Office (LCSO) establishing that the victim had

been defrauded out of over $5 million between in or around April 2024 and in or around July 2024 in a Pig Butchering scheme.

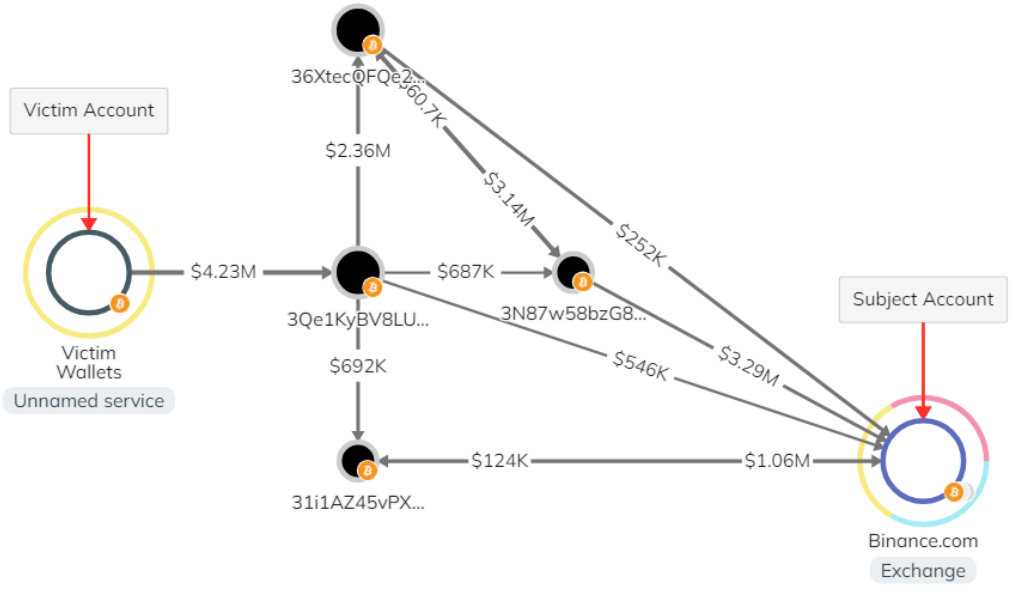
22. In or around April 2024, the victim met the unknown subject(s), purportedly a woman named Amy Pan (Pan) via text message. The victim received an unsolicited text message from Pan stating "We are going to Central Park tomorrow. Do you want to come with us?" The victim replied, jokingly (as the victim described), "Sure, but I don't know who you are. Plus I don't know if I can be in New York by tomorrow." Pan apologized, and the two continued exchanging text messages. Pan then suggested to move the conversation to WhatsApp, which the victim agreed to do. During their conversation on WhatsApp, Pan claimed to be knowledgeable about short-term cryptocurrency trading and eventually convinced the victim to begin investing, with the assistance of Pan.

23. Pan walked the victim through setting up accounts at Kraken and Strike, which are cryptocurrency exchanges. The victim already had an account at Coinbase, which is another cryptocurrency exchange. Pan walked the victim through how to link his accounts. Pan explained that the victim could use his various cryptocurrency exchange accounts to purchase cryptocurrency and then move that cryptocurrency into a trading platform called Wealthob.com (“Wealthob”). The investigation revealed that the domain Wealthob.com was created on or about April 1, 2024, just shortly before Pan began engaging with the victim.

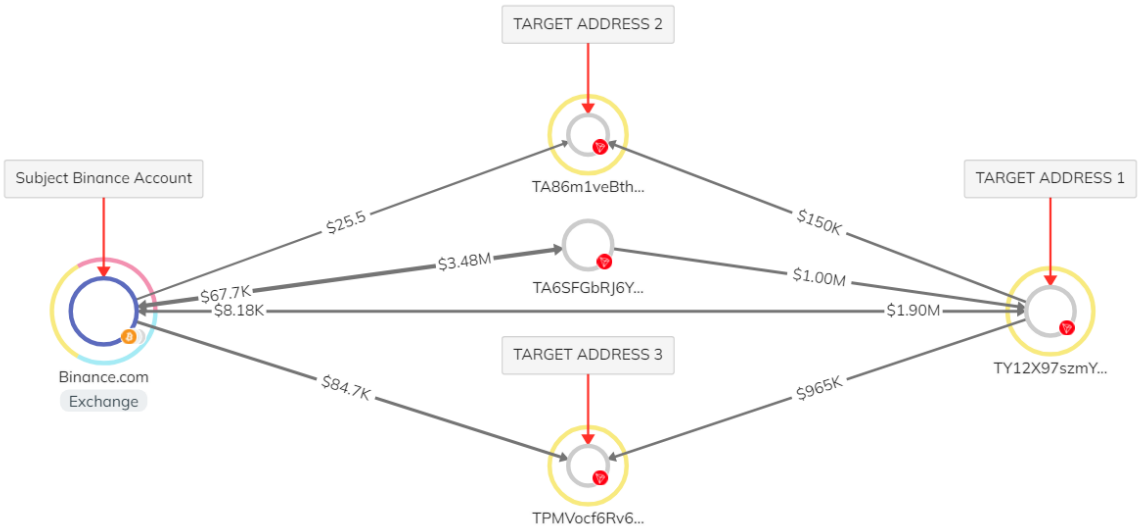
24. In or around April 2024, at the direction of Pan, the victim made an investment account at Wealthob. Starting in or around April 2024, at Pan’s direction, the victim began sending money from his various cryptocurrency exchange accounts to what he believed was his wallet at Wealthob. Pan then began “teaching” the victim how to trade within his Wealthob

account. In just seconds, the victim believed he made $300 on a trade. Pan then showed the victim how he could make a withdrawal, which is a common tactic used in these types of investment fraud schemes – lead the victim to believe they have made money trading, let them withdraw a small amount, and then encourage them to invest more funds. At this point, Pan knew, based on what the victim had told her, that the victim had access to nearly $7 million.

25. Between in or around April through in or around July 2024, the victim sent over $5 million worth of BTC and ETH to what the victim believed was his Wealthob account. The majority of the funds, approximately $4.2 million, were sent from the victim's Strike account, via BTC, to wallet address 3Qe1KyBV8LUE5tQuKhgVqbGVqcF2KNByk2 ("3Qe1K"), which is unrelated to any legitimate trading platform. This BTC was then sent by the individual(s) with control of this wallet to other wallets, and eventually transferred to wallets at Binance.com, as illustrated below.



26. Binance.com records identified the account was associated with user ID 816682606 and belonged to a female in China named 康秀花 (translated to Yasuhide Flower) (hereinafter "BINANCE ACCOUNT # 816682606"). BINANCE ACCOUNT # 816682606's transaction history showed that it converted the BTC into USDT and moved it to various wallets, including the three cryptocurrency addresses associated with the Defendant Property ("the three addresses"), as illustrated below.



27. The following transactions are select examples of the movement of victim funds to the three wallet addresses. Due to the volume of transactions, and for purposes of this complaint, not all transactions are detailed below.

May 24, 2024, through July 9, 2024

28. On or about May 24, 2024, at approximately 19:24 UTC, the victim transferred approximately 10.08 BTC (valued at approximately $695,263) from his Strike account to 3Qe1K.

29. On or about May 25, 2024, at approximately 04:09 UTC, less than 9 hours later, approximately 10 BTC (valued at approximately $687,423) was transferred from 3Qe1K to 3N87w58bzG8aUZzvD5BKxZjqRVyj7SkKvA ("3N87w"), an address controlled by the individual(s) behind the scam, where it was comingled with other funds from 36XtecQFQe2YDpBhoh7Rw26LSF13CEHFtU ("36Xtec"), which also held victim funds. The deposit of 10 BTC into 3N87w was the first deposit transaction into this wallet address.

30. On or about May 29, 2024, at approximately 23:07 UTC, the victim transferred approximately 8.8 BTC (valued at approximately $594,923) from his Strike account to 3Qe1K.

31. On or about May 30, 2024, at approximately 02:30 UTC, about 3.5 hours later, approximately 8.8 BTC (valued at approximately $597,986) was transferred from 3Qe1K to 36Xtec, an address controlled by the individual(s) behind the scam, where it was comingled with other funds.

32. On or about May 30, 2024, at approximately 04:49 UTC, about two hours later, approximately 10 BTC (valued at approximately $681,539) was transferred from 36Xtec to 3N87w.

33. On or about June 5, 2024, after receiving victim funds from 3Qe1K and 36Xtec, approximately 27 BTC (valued at approximately $1,916,985) was transferred from 3N87w to 1DXmVoKLEXDjCWqwBwmSVzs17WJN3uvaeW ("1DXmV"), which is a wallet hosted by Binance.com and belonging to Yasuhide Flower, BINANCE ACCOUNT # 816682606.

34. On or about June 5, 2024, after converting BTC to USDT, BINANCE ACCOUNT # 816682606 sent approximately 1,901,366 USDT (valued at approximately $1,901,556) to TY12X97szmYzYAmYLsh86cbYfh9psufgeV ("fgeV").

35. On June 7, 2024, approximately 190,000 USDT (valued at approximately $189,867) was transferred from fgeV 1 to TPMVocf6Rv6bMLnRMX4RXoriiTbT9P82k2 ("82k2"). Of note, no other funds were deposited to fgeV between June 5, 2024, and July 9, 2024, making it clear that the funds transferred to 82k2 were derived from the victim's funds.

36. On July 8, 2024, approximately 775,000 USDT (valued at approximately $775,000) was transferred from fgeV to 82k2. Of note, no other funds were deposited to fgeV between June 5, 2024, and July 9, 2024, making it clear that the funds transferred to 82k2were derived from the victim's funds.

37. On July 9, 2024, approximately 149,990 USDT (valued at approximately $150,005) was transferred from fgeV to TA86m1veBthXyvXcN1mDixgYNXChkMjhh ("Mjhh"). Of note, no other funds were deposited to fgeV between June 5, 2024, and July 9, 2024, making it clear that the funds transferred to Mjhh were derived from the victim's funds.

The THREE WALLETADDRESSES

38. FgeV was first created on or about February 25, 2024, and was active through on or about August 3, 2024.

39. Over the course of this timespan, fgeV has received approximately 3,607,426 USDT, which is roughly equivalent to $3,608,222.88 USD. Of that, approximately $2.9 million received by fgeV has been received, either directly or indirectly, from BINANCE ACCOUNT # 816682606.

40. Mjhh was first created on or about July 8, 2024, and was active through on or about July 27, 2024.

41. Over the course of this timespan, Mjhh has received approximately 150,013 USDT, which is roughly equivalent to $150,028.68 USD. Of that, approximately $150,015 received by Mjhh has been received directly from fgeV.

42. 82k2 was first created on or about November 10, 2022, and was active through August 9, 2024.

43. Over the course of this timespan, 82k2 has received approximately 1,354,158.51 USDT, which is roughly equivalent to $1,354,148.30 USD. Of that, approximately $965,000 received by 82k2 has been received directly from fgeV.

44. There is no reason, economic or otherwise, for legitimate businesses or individuals to conduct cryptocurrency transfers in the above fashion. Whether transferring BTC or, in this case, USDT, each individual cryptocurrency transfer costs money. For USDT, that cost is paid via "gas" fees levied by operation of Ethereum blockchain. Businesses and individuals who simply seek to transfer legitimate funds from one address to another strive to minimize those fees by conducting transfers with as few transactions, or "hops," as possible.

45. The convoluted transactions and quick swaps from one type of cryptocurrency to another described above indicate that the motivation behind the transactions is to conceal the nature, origin, location, control, and ownership of the funds.

The Victim Discovers He is Being Scammed

46. On or about June 30, 2024, the victim attempted to withdraw funds from his Wealthob account. However, upon attempting to withdraw funds, the victim was told he needed to pay taxes on the profits, which is a common tactic in these schemes as an attempt to get more

money from victims. The victim was told that his profit was 20,604,636.4 USDT and that he needed to pay taxes of 1,957,440.46 USDT.

47. The victim then contacted his financial advisor and explained he needed to liquidate his savings to pay the tax. The victim's financial advisor immediately suspected the victim was being scammed and advised him to report it to law enforcement.

48. On or about July 9, 2024, the victim submitted a complaint to the FBI and also reported it to LCSO. Tracing of the victim's transactions shows that the cryptocurrency was not placed in the victim's investment account at Wealthob; rather, it was laundered through multiple wallets before being deposited in the three wallet addresses.

49. As the funds currently held in the three wallet addresses are involved in money laundering, the funds are subject to forfeiture. While the victim transfers may have been sent to other wallets as BTC, any USDT located within the three wallet addresses constitutes property involved in money laundering as it helped conceal the nature, source, location, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

50. On or about July 29, 2024, LCSO sent a request to Tether asking for a voluntary freeze of the Defendant Property in the three wallet addresses.

51. On or about July 30, 2024, Tether confirmed they had frozen the three wallet addresses and informed LCSO of the following balances:

a. fgeV: 852,654.047192 USDT

b. Mjhh: 105,553.680342 USDT

c. 82k2: 1,013,192.066449 USDT

52. Financial tracing of these three wallet addresses showed that no other significant amount of funds was transferred into them between receiving victim funds and being frozen by Tether, further indicating that the frozen amounts are indeed victim funds.

53. Ultimately, the FBI obtained a lawful seizure warrant for the contents of the three wallet addresses on December 6, 2024.

FIRST CLAIM FOR RELIEF
(Forfeiture under 18 U.S.C. § 981(a)(1)(A))

54. The United States incorporates by reference paragraphs 1 – 53 above as if fully set forth herein.

55. Title 18, United States Code, Section 981(a)(1)(A) subjects to forfeiture "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . of this title, or any property traceable to such property."

56. Title 18, United States Code, Section 1956(a)(1)(B)(i) imposes criminal liability on "[w]hoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity . . . knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity."

57. As set forth above, the Defendant Property constitutes property involved in a violation of section 1956.

58. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

SECOND CLAIM FOR RELIEF
(Forfeiture under 18 U.S.C. § 981(a)(1)(C))

59. The United States incorporates by reference paragraphs 1 – 53 above as if fully set forth herein.

60. Title 18, United States Code, Section 981(a)(1)(C) subjects to forfeiture "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting 'specified unlawful activity' (as defined in section n1956(c)(7) of this title) or a conspiracy to commit such offense."

61. Title 18, United States Code, Section 1956(c)(7)(D) provides that the term "specified unlawful activity" includes "an offense under . . . section 1343 (relating to wire fraud)."

62. As set forth above, the Defendant Funds constitute criminal proceeds of the wire fraud scheme.

63. As such, the Defendant Funds are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C).

PRAYER FOR RELIEF

WHEREFORE, the United States prays that due process issue to enforce the forfeiture of the Defendant Funds and that due notice be given to all interested parties to appear and show cause why said forfeiture of the Defendant Funds should not be decreed, that the Defendant Funds be condemned and forfeited to the United States to be disposed of according to law, and for such other and further relief as this Honorable Court may deem just and proper.

DATED this 27 day of March 2025.

Respectfully submitted,

ERIK S. SIEBERT
UNITED STATES ATTORNEY

By: /s/Annie Zanobini

Annie Zanobini
Assistant United States Attorney
California Bar No. 321324
2100 Jamieson Avenue
Alexandria, Virginia 22314
Office Number: (703) 299-3903
Facsimile Number: (703) 299-3982
Email Address: annie.zanobini2@usdoj.gov

VERIFICATION

I, Jamie Daly, Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury as provided by 28 U.S.C. § 1746, that the foregoing Complaint for Forfeiture in Rem is based on information known by me personally and/or furnished to me by various federal, state, and local law enforcement agencies, and that everything contained herein is true and correct to the best of my knowledge.

Executed at Manassas, Virginia, this 27th day of March 2025

Jamie Daly

Jamie Daly, Special Agent
Federal Bureau of Investigation